Introduction

This document is an **independent review** of the **claims**, **legal documentation**, and **verification process** of the child-focused identity verification service k-ID, which is partnered with popular platforms and games such as **Discord** and **Gorilla Tag,** among many others.

In this document, we *("we" will be used without detail as we wish to remain anonymous. If any party claims authorship of this document, it is best to treat it as false.)* review a distressing number of seemingly **open-ended**, **vague**, and **potentially dangerous** clauses in both the Privacy Policy and Terms of Service of k-ID, as well as commentary on the **trustworthiness** of the identity verification *partners* they work with.

As we are not legal professionals, treat everything in this document as *alleged* unless otherwise confirmed by k-ID. *We've included links and contextual quotes where possible to ensure you can follow along with our analysis, and have an interpretation for yourself of k-ID's own documents.*

We have found what we believe are **multiple potential issues** with k-ID that could allegedly put the **safety**, **privacy**, and **security** of children, and their parents' personal information, **including biometric data and government issued ID**, at risk, through a number of possible threats, while also **not seeming to actually verify users' identities**, the primary thing k-ID is meant to do.

Some of the issues we will discuss include:

- **Vague language** around which companies your data is **shared with**, and in what manner
- Attempting to **prevent independent security audits** of their service
- Possibly allowing for future **leakage of personal information** in **advertising** and **generated datasets**
- Allowing for the **transfer of personal information across borders** to areas with **worse privacy laws**
- Permanently **stripping your right to sue them in a class action** (and **capping** some damages at just **$100**)
- and **much more.**

Do note that while we have conducted a thorough investigation across as much of the service as we can access, **we are limited in our capacity to fully analyze the internal workings of k-ID**, as we don't have any internal access, or ability to use industry standard forensic tools without possible legal consequences.

While we would have liked to reach out to k-ID directly for comment before publishing this document, in order to *protect ourselves from the aforementioned possible legal complications,* we've decided to publish this document anonymously in case k-ID decides that a cursory attempt at accessing publicly available domains is considered an "attempt to probe, **scan or test the vulnerability of any our system or network**," which is against their Terms of Service.

The "Covering Up Potential Security Vulnerabilities" section of this document includes more context regarding that possibility.

All of our commentary is based on current documentation from k-ID and their verification partners' websites and code repositories as of 5/17/2025.

If you'd like further details, read below.

Untrustworthy Identity Verification Partners

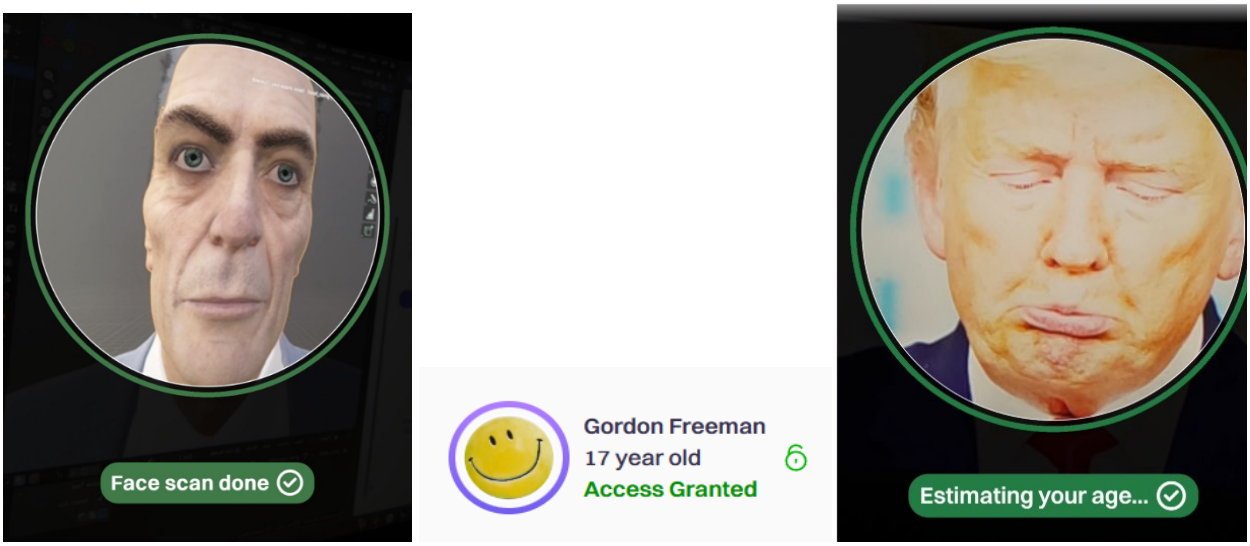
k-ID's Terms of Service & Privacy Policy **don't explicitly mention which partners for identify verification they work with or transfer data to.** Only a few are found in the *Cookies Policy* of all places, and it's unclear if this is actually the **only** companies your data could be transferred to, **or if others exist.**

Issues With Veratad Verification

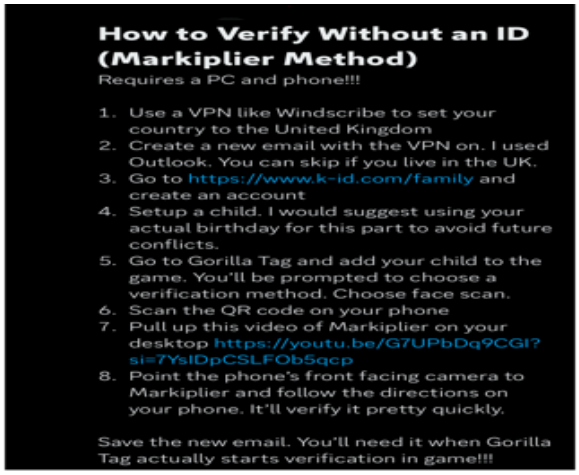
The **first** of the identity verification partners they seem to partner with is Veratad, (AKA dcams.app) which has been **sued** before for **allegedly transferring biometric data to other companies without consent.**

Veratad is not a small company, either. They also work with companies like **JUUL**, among others *(including a major tobacco company, and large corporations such as T-Mobile and Epic Games).*

Veratad's verification system, seemingly implemented as **K-ID's core age verification mechanism** in many areas, has already been **trivially bypassed**, using methods as simple as, when asked for picture of your face to prove age, pointing the phone at an easily manipulated **3D model** in the popular free software Blender, or **video of the United States President...**



...or a YouTube video from the popular YouTuber Markiplier, which has become a popular and documented method, with a currently uncountable number of children allegedly successfully verifying their accounts on the platform using it.


How to Verify Without an ID (Markiplier Method)
Requires a PC and phone!!!
1. Use a VPN like Windscribe to set your country to the United Kingdom
2. Create a new email with the VPN on. I used Outlook. You can skip if you live in the UK.
3. Go to https://www.k-id.com/family and create an account
4. Setup a child. I would suggest using your actual birthday for this part to avoid future conflicts.
5. Go to Gorilla Tag and add your child to the game. You'll be prompted to choose a verification method. Choose face scan.
6. Scan the QR code on your phone
7. Pull up this video of Markiplier on your desktop https://youtu.be/G7UPbDq9CGI?si=7YsIDpCSLFOb5qcp
8. Point the phone's front facing camera to Markiplier and follow the directions on your phone. It'll verify it pretty quickly.
Save the new email. You'll need it when Gorilla Tag actually starts verification in game!!!

This is something **most other identity providers are not vulnerable to**, and this **seriously raises into question Veratad's trustworthiness.**

Keep in mind that they work with companies like JUUL, and a major tobacco company, so if this issue stems from *their* technology rather than k-ID's implementation, this could be a serious issue legally for the entire company.

Veratad states they have technology to prevent this, stating

> **"certified liveness detection lets you quickly match individuals to records while preventing spoofing.** Selfie fraudsters need not apply."

...but it seems that may not be the case.

This could carry large implications not just for the fundamental business and legal compliance case of k-ID, but also for the **safety of children, who, when their parents believe k-ID is properly vetting**

all users, may not supervise their children on "child-safe" platforms, that then allow people on who are not of the correct age after they bypass the verification system in place.

Possible Legal Implications of Geolocation Alteration

It also seems that the user's **location,** which determines *which verification methods are used,* is based solely on **IP address location,** which is **trivially bypassed with a VPN,** according to many public attempts we've seen to verify without ID online.

This could possibly be violating data verification laws in some regions.

Most identity verification services require an IP address that is **not flagged as being from a server hosting organization or datacenter for verification** to prevent this exact issue, and the fact such a check seemingly doesn't exist seems to put the quality of the service into question even further.

Potentially Shady Practices Within Microblink

k-ID also partners with Microblink, which seems to state that companies can effectively **alter the likelihood of a potentially suspicious account being approved...**

> The balance of false acceptance rate with the rate of false rejections should be in your control, **based on how your business balances growth ambitions versus fraud risk.** The Microblink Platform lets you **customize the decision threshold for each verification check in a few clicks.**

This could possibly cause k-ID to violate any number of identity verification requirements, should they set this threshold low enough that it causes someone who shouldn't be allowed on the services to join. (*We weren't able to find any policy or document relating to how high or low k-ID sets this threshold, if they adjust it at all. We believe k-ID should be more transparent about this.)*

Increased Risk of Vulnerabilities

We've noticed many practices that seem like they increase the possibility that k-ID could be vulnerable to a future exploit, that could potentially release customer information.

Unauthenticated Staging Domains

k-ID seems to have three **staging/preview subdomains** (testing sites that, in some cases, can **include out-of-date, and/or vulnerable code**) that are *still public*, with *no prior authentication*, some of which have **login & account creation forms** accessible.

When staging domains have forms that can be submitted, this can increase the likelihood that an exploit will be possible, which could hypothetically risk other data on the service.

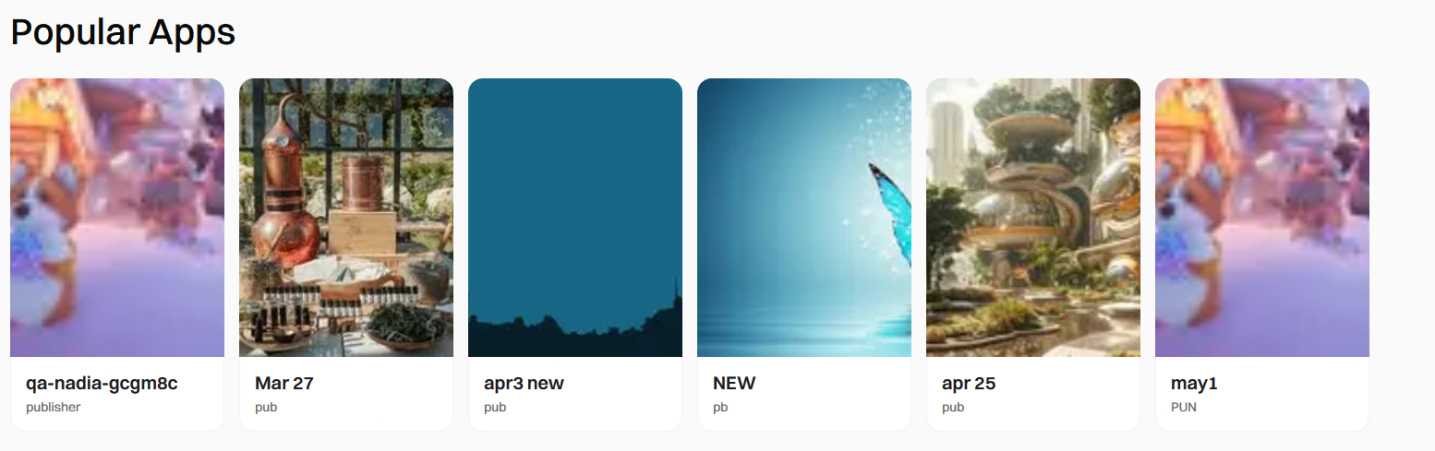
These domains were found via publicly available sources, namely certificate transparency, and would be easily visible to any bad actor.

- https://family.staging.k-id.com/
- https://portal.staging.k-id.com/login

- https://family.preview.k-id.com/
- (*multiple have been taken offline recently, however. There used to be many more.*)

These domains show incomplete, unpolished mock game listings, and it's unclear how long ago they were created, or if they are currently running the most up-to-date, secure versions of k-ID's internal software.

We hope they are, but as you'll see later, we aren't allowed to test for ourselves.



Preventing Third-Party Audits

k-ID explicitly states that you are **not allowed to:**

> "Attempt to probe, **scan or test the vulnerability of any our system or network** or breach any security or authentication measures"

Most companies **welcome** attempts at finding vulnerabilities, because it keeps them more secure. People doing free work to check your security is generally a good thing to have. In fact, this is often so valuable to the security of a company, that many companies **pay** for vulnerabilities found *(bug bounties)*

However, k-ID seems to rejects this trend, and it appears they're trying to **prevent people from engaging in tests of their security.**

On a personal, opinionated note from one of the authors: As an independent security researcher, when someone tells you not to look for flaws in their system, and to just take their word for it, **it *often* means they're not confident in their system's security.** While this isn't a guarantee of insecurity, it does increase the likelihood, in my opinion.

Potential Unsafe Data Handling

k-ID claims to take data security very seriously. However, we have reason to believe that **vague language**, potentially **bad data handling practices**, and **deliberate release of customer information** could lead to data leaks, re-identification of personal data, and more.

k-ID claims that:

> "k-ID does NOT store the information we collect and use to validate your age or parent/guardian status. **All we store is the result of the validation process (i.e., whether you passed or failed).**"

However, you may notice that this only states if they **store** data, but not if they act as a proxy, middleman, or otherwise third party involved in the **handling** of your data between you, and the identity verification service, which could pose a risk if they are.

While we hope k-ID is not acting as a middleman in this process, **we would appreciate if k-ID clarified their policies regarding this to eliminate that possibility, if it is indeed true.**

Global Transfer & Storage

According to k-ID's policies, **any** information you provide to k-ID for processing can be:

> "All information processed by us may be transferred, processed, and stored **anywhere in the world**, including, but not limited to, the United States or other countries, **which may have data protection laws that are different from the laws where you live.**"

This means they could potentially store your personal information in a region in which **data protection laws are minimal,** and are more likely to risk your information being available in a future data breach.

They claim they "endeavor to safeguard your information." However, **that doesn't appear to be a legally binding commitment.**

As mentioned before, it doesn't seem that this data would necessarily include biometric or ID information, however it could potentially include other details you provide to them. Think things like email, phone number, name, address, family structure if you've added kids to your family portal, etc.

"De-Identification"

k-ID also states that:

> "we may use personal information to create **de-identified** and/or aggregated information"

They then *only* give an example of **aggregated** information (e.g. x users use the platform) while conveniently leaving out anything regarding **de-identified** information, which is notoriously easy to **re-identify.**

k-ID **doesn't state what specific information they would remove** to consider your data "de-identified," which opens up the **possibility of your data being re-identified at a later date,** should they provide "de-identified" data to a third party.

Using Your Information in Marketing Material

They also reserve the right to **use your name and "logo" (likely to be a profile picture of people's face or in-game avatar) in marketing material.**

> "We reserve the right to feature your name and logo as a user of our Services on our platforms and promotional materials."

We believe k-ID should <u>always</u> ask for explicit consent before doing this, and require that they do such in their policies before it is legal for them to do so.

"Necessary" Sharing

k-ID additionally appears to **allow themselves to share your information** with **any service provider or partner** they feel is "necessary" to provide the services.

This can sometimes be unnecessarily broad, and could hypothetically lead to them deeming a transfer of your personal information "necessary," **<u>even if it's not.</u>**

This additionally, from what we can see, has **no clause that would require them to notify you if your information was shared with a service provider or partner that you were not previously aware of.**

While **this language isn't always *inherently dangerous***,it could be risky depending on how k-ID decides to **interpret** the term "necessary" with regard to actions they might take with user information.

Potential Future Sale of Data

k-ID claims *not to hold onto sensitive data longer than they need it*, **which is commendable.** They even partnered with the **ESRB Privacy Certified initiative** for third-party auditing, which we believe is a strong step in the right direction.

However, not only is this policy **difficult to enforce consistently**, especially in a company that is relatively new, and rapidly changing, and even slightly misconfigured logging software can **accidentally store sensitive information**, but it's also unclear **exactly** how long they maintain your personal information *(and which specific information is being held)* before it's no longer "necessary" to provide the service.

While we do believe it's unlikely k-ID is secretly holding on to data well past when they claim they need to use it, we would like more clarity as to the exact duration of time data is kept, and more transparent communication to end users on when their data has been successfully removed.

In a system in which k-ID could be processing and storing personal information, whether that be an ID and face scan, or simply full names and contact information, transparency is key.

k-ID claims they won't sell your personal information.

Except, they gave themselves the ability to if they so choose to sell the company... *(which is not abnormal in itself, as to sell a company means selling the corresponding account data so the service doesn't start over from scratch)*

> "your information may be sold or transferred in connection with such a transaction"

or **move their services to another provider.**

> "**transition of service to another provider**,"

...which could be **extremely broad** if used in the wrong way, as it could allegedly allow them to sell or transfer your information simply if they were to move service providers, again, as long as they deem it

"necessary." **This needs more clarity, and we'd ideally like to see more detail regarding what data this includes, what situations it would be allowed, and what data protection said provider must have in place for data to be transferred.**

They also specify that they don't **currently** engage in sales of your data.

> "Note that we do not **currently** engage in any targeted advertising or data sales"

Which, while possibly just being something that's up to interpretation, doesn't exactly inspire confidence in them **never** doing so.

We would like to see an explicit commitment to never selling or transferring any customer information for the purposes of advertising, permanently.

Overly Broad Content Licensing

k-ID also appears to get the legal right to do **nearly anything they wish with user content you upload,** stating that you give them and their partners:

> "a license to **use**, modify, **distribute**, and create derivative works from it. This license is non-exclusive, **perpetual**, and worldwide. We can use your User Content to operate, provide, **promote**, and improve our Services."

This does not include meaningful, explicitly defined language defining **what data of yours** could or could not be included here, such as data you upload that identifies yourself, or personal information such as identifiers, contact details, etc.

We don't know what particular data this includes, and **we believe this needs to be clarified further by k-ID.**

Waiving of Your Legal Rights

This is unfortunately something many companies are doing nowadays, and it's disappointing to see k-ID continuing this practice. **Waiving the legal rights of your users to insulate your company from what could very well be justified legal action in the future is a dangerous precedent**, and we believe k-ID should retract these policies immediately for the safety of their users.

Waiving Your Right to a Class Action Lawsuit

When sign up for an account on k-ID's site, you **waive your right to sue them in a class action lawsuit.**

This is not hyperbole. If you make an account, **you cannot band together with other people who were harmed by them in the future, and sue them:**

> "We both agree to solve any disagreement through individual arbitration, rather than in a group or consolidated action. The U.S. Federal Arbitration Act will govern how we interpret and enforce this agreement. By agreeing to this, **we are giving up our right to a trial by jury or to participate in a class action."**

And **even if you delete your account,** your right to sue them in a class action is **permanently** gone.

> "This agreement will **continue even after our agreement ends.**"

The only time this restriction seemingly doesn't apply is when your case applies for **small claims** court...

...or through the **exemption they made for themselves** in the case of anybody illegally using their intellectual property.

> we can still go to court to get an injunction if someone is infringing on our intellectual property rights.

Limiting Damages Owed

k-ID also seemingly attempts to **limit certain damages owed to you to just $100.**

> "we and our service providers are not responsible for any damages, including incidental, special, exemplary, or consequential damages, or for lost profits, revenues, savings, business opportunities, data, or goodwill, or for service interruptions, computer damage, or system failure, or for the cost of substitute services of any kind arising from or related to these terms or the use of the services, whether based on warranty, contract, tort, product liability, or any other legal theory. **Our total liability for these terms or the use of the services will not exceed the amounts you have paid or owe us for the services, or $100** if you have not had any payment obligations to us."

And this seemingly only excludes a few possible worst-case scenarios:

> However, we are still liable for losses that cannot be excluded or limited by applicable law, such as **death** or **personal injury** caused by our **negligence or fraud.**

Absolving Employees of Responsibility

You also **indemnify and hold all their employees harmless from any claims, disputes, demands, liabilities, damages, or losses.**

> "You will indemnify and hold us and our officers, directors, employees and agents, harmless from and against any claims, disputes, demands, liabilities, damages, losses, and costs and expenses, including, reasonable legal and accounting fees arising out of or in any way connected with (a) your access to or use of the services, (b) your User Content, or (c) your violation of these Terms."

Vague Language

Something that we've consistently observed throughout k-ID's policies is a lack of concrete, highly descriptive language regarding the exact details of how data is used.

While it's often useful to users to have a more simple, all-encompassing policy that covers more of the service broadly from a readability perspective, **it also harms the ability of users to know how exactly their data is being used.**

We would like k-ID to provide more clear wording regarding how specifically each type of data is used, how long it's stored, which specific, named entities it can or will be transferred to, and the exact purpose of processing for each type of data, instead of stating broad categories of entities, general types of use, and as you'll see below, vague language that could make it hard for users to tell what specific data of theirs could be sent to which specific companies, or used for which specific purpose.

"Includes" Means More Than What it Claims

k-ID seems to **expand much of their previous language** by stating that:

> The usage of terms such as “includes”, “including”, and “such as” should not be considered as an exhaustive list, and **other items may also be included.**

This is a great example of how we wish k-ID would be more specific and methodical in choosing exactly who, where, and how user data is transferred, to avoid the possibility of data being transferred to entities that users **previously did not believe** were within the scope of the policies.

Note From The Authors

k-ID is attempting to solve a problem, and **we understand that.** *Kids should be able to safely play games with proper parental controls in place, and we commend k-ID for attempting to create a safe online experience for parents and their children.*

But solving the problem of underage kids being exposed to unsafe content in games is not done by allegedly **processing the government IDs or biometric data of adults or possibly children** through a provider that doesn't seem to do what they claim, then **potentially storing it in an unsafe manner,** while being **vague about who the information could be shared with,** and attempting to **reduce the amount of scrutiny on the service's security** in the process.

Not only does processing such a large volume of personal information make k-ID a great target for bad actors, which necessitates **extreme precautions and very clear policies,** but in its current state, k-ID seems to fund identity verification companies that are seemingly providing low quality, or even outright nonfunctional identity and age verification services under the guise of protecting children. This **potentially risks the safety and privacy of parents, and their children.**

In the opinion of the authors of this paper, if online games and services are to use identity and age verification services, these services must properly **protect** user data, have **extensive publicized legal agreements,** and collect only the **very minimum** amount of data necessary to do their job, while ensuring **transparency** about data **collection, transfer, and storage** throughout the whole process.

Every transfer and action taken upon anybody's personal data should be **extremely well documented**, and any user should be **notified immediately** if their data is, will, or has been **transferred to a third party.**

We do not personally believe k-ID meets these standards, and as such, *we would not use, or recommend using k-ID's services until k-ID:*

1. **Clarifies** unclear language in their policies.
2. Makes a **public statement** explaining their **commitment to user privacy.**
3. **Reduces restrictions** on third-party verification of their service's **safety.**
4. **Increases transparency** as to the data they collect, store, and disseminate, not just to individual users, but to the public.
5. Ensures their verification partners aren't **vulnerable to trivial bypasses.**
6. Explains why their users must be **prevented from suing them** in a class action lawsuit, or preferably, *removes the forced arbitration clause entirely.*

We understand that some current users of k-ID may be concerned.

If you would like to **delete** the information that k-ID does allow you to delete from their service, you can contact them at **privacy@k-id.com**, or through the Parent Portal, under "Help."

If a game or service you or your child uses *is or has implemented k-ID*, **you may want to contact them** to request that they reconsider their partnership with k-ID **until these issues have been addressed,** and if you are a parent, prevent your child from using k-ID **until you believe the k-ID meets your standards for a safe, private, and secure platform that you'd trust your child's information on.**

If you are a journalist, content creator, or otherwise seeking comment from us, you can reach us at the email alias ***kid.hatless337@8shield.net***

(This email may not be active, monitored, or in existence in the future, should it receive too much spam, or otherwise become unmanageable or irrelevant. Do not consider this a guaranteed method of contact.)

For Content Creators:

We sincerely encourage you to share this document along with videos you may release on the matter, with fellow creators, and with your communities. If you've taken the time to read this, consider ensuring this important discussion does not get ignored in the inboxes of other creators, spread the message, and keep the games and platforms you've built your community on safe from dangerous practices that k-ID could be engaging in.

We're aware that many of the creators that will have the most influence at the moment will be those who make content on Gorilla Tag, which is implementing k-ID. This could impact a very large quantity of players, and we especially encourage any Gorilla Tag focused creators to spread this message to ensure that players' personal data and online safety remain intact.